Adage:

Authorization for Distributed Applications and Groups

Mary Ellen Zurko
OSF Research Institute
zurko@osf.org
http://www.osf.org/~zurko/
http://www.osf.org/www/adage/

Adage Motivation

Current Problems

Complex administration

- Tools are low-level (ACLs)
- Poor tools for grouping large numbers of subjects/objects

Inconsistent mechanisms across applications

Limited notions of distributed trust

- No tools for high-level policy statement
- Only highly structured or anarchic trust infrastructure and only for authentication

Adage Context

Secure Distributed Authorization

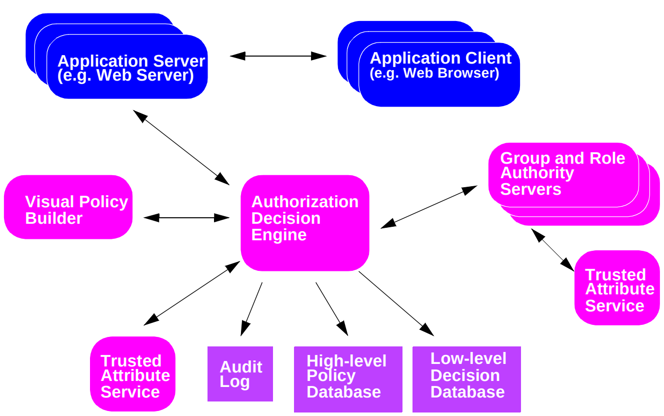
Goals:

- Emphasis on communication within a single geographically distributed organization
- Policy-neutral: Applicable to multiple environments
- “User-friendly security” is not an oxymoron

Non-goals:

- Integrity, privacy, or authentication research
- Applicability to global, unmanaged environments

Adage Architecture



Authorization Tools

Visual Policy Builder for High Level Authorization Language

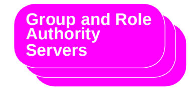
Inputs include

- user and object attributes (names, groups, roles, labels, ownership)
- contextual information (transaction history, time)

High-level Security Policy Database

- Platform-independent policy representation
- Sharing of policy primitives between organizations

Group and Role Authority Server (GRAS)



Support for groups and roles with rich semantics, including relationships and restrictions between them

Types of groups and roles derived from models and policies in the security and groupware literature

Multiple group authorities hold different group memberships for a single authenticated identity

A single enforcement engine manages authorization and group information

Trust Model

Framework for users to think about and use authorization for organizational policies

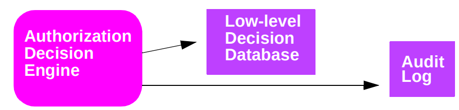
Underlying model provides a consistent foundation for common trust dimensions

- Supports notions of amount and kind of trust and trusted referrals

Trust model matches user expectations about how security should work

- Security, performance and usability trade-offs

Enforcement Engine



Underlies all of the Adage components

Low-level Authorization Decision Database

- Platform-dependent policy representation
- Contains low level representation of authorization data, such as ACLs
- Performance sensitive to application needs

Auditing support